Release Notes for Cisco Wireless Controllers and Lightweight Access Points, Cisco Wireless Release 8.10.105.0

First Published: 2019-10-19

Last Modified: 2022-08-30

About the Release Notes

This release notes document describes what is new or changed in this release, instructions to upgrade to this release, and provides information about the open and resolved caveats for this release. Unless otherwise noted, in this document, Cisco Wireless Controllers are referred to as *controllers*, and Cisco lightweight access points are referred to as *access points* or *APs*.

Revision History

Table 1: Revision History

Modification Date	Modification Details
August 30, 2022	Added: Supported VIDs for Cisco Catalyst 9130 Access Points and Cisco Catalyst 9120 Access Points
April 30, 2020	Updated: **CIMC Utility Upgrade for 5520 and 8540 Controllers** section—Included 3.x and 4.x recommended CIMC version upgrade.

Supported Cisco Wireless Controller Platforms

The following controller platforms are supported in this release:

- Cisco 3504 Wireless Controller
- Cisco 5520 Wireless Controller
- Cisco 8540 Wireless Controller
- Cisco Virtual Wireless Controller (vWLC) on the following platforms:
  - VMware vSphere Hypervisor (ESXi) Version 5.x and 6.x
  - Hyper-V on Microsoft Server 2012 and later versions (support introduced in Release 8.4)
  - Kernel-based virtual machine (KVM) (support introduced in Release 8.1). After KVM is deployed, we recommend that you do not downgrade to a Cisco Wireless release that is earlier than Release 8.1).

- Cisco Wireless Controllers for High Availability for Cisco 3504 Wireless Controller, Cisco 5520 Wireless Controller, and Cisco 8540 Wireless Controller
- Cisco Mobility Express

Note In a network that includes Cisco Catalyst Center (formerly Cisco DNA Center) and Cisco AireOS controller, and the controller fails provisioning with **Error NA serv CA certificate file transfer failed** error, as a workaround, we recommend you reboot the affected AireOS controller.

Supported Cisco Access Point Platforms

The following Cisco AP platforms are supported in this release:

- Cisco Catalyst 9130 Access Points
  - C9130AXI: VID 02 and earlier
- Cisco Catalyst 9120 Access Points
  - C9120AXI: VID 06 and earlier
  - C9120AXE: VID 06 and earlier
  - C9120AXP: All VIDs
- Cisco Catalyst 9117 Access Points
- Cisco Catalyst 9115 Access Points
- Cisco Aironet 700 Series Access Points
- Cisco Aironet 700W Series Access Points
- Cisco AP803 Integrated Access Point
- Integrated Access Point on Cisco 1100, 1101, and 1109 Integrated Services Routers
- Cisco Aironet 1700 Series Access Points
- Cisco Aironet 1800 Series Access Points
- Cisco Aironet 1810 Series OfficeExtend Access Points
- Cisco Aironet 1810W Series Access Points
- Cisco Aironet 1815 Series Access Points
- Cisco Aironet 1830 Series Access Points
- Cisco Aironet 1840 Series Access Points
- Cisco Aironet 1850 Series Access Points
- Cisco Aironet 2700 Series Access Points

- Cisco Aironet 2800 Series Access Points
- Cisco Aironet 3700 Series Access Points
- Cisco Aironet 3800 Series Access Points
- Cisco Aironet 4800 Series Access Points
- Cisco ASA 5506W-AP702
- Cisco Aironet 1530 Series Access Points
- Cisco Aironet 1540 Series Access Points
- Cisco Aironet 1560 Series Access Points
- Cisco Aironet 1570 Series Access Points
- Cisco Industrial Wireless 3700 Series Access Points
- Cisco Catalyst IW6300 Heavy Duty Series Access Points
- Cisco 6300 Series Embedded Services Access Points

Note

- Cisco AP803 is an integrated access point module on the Cisco 800 Series Integrated Services Routers (ISRs). For more information about the stock-keeping units (SKUs) for the AP803 Cisco ISRs, see:

  http://www.cisco.com/c/en/us/products/routers/800-series-routers/brochure-listing.html.

- For more information about Integrated Access Point on Cisco 1100 ISR, see the product data sheet:

  https://www.cisco.com/c/en/us/products/collateral/routers/1000-series-integrated-services-routers-isr/datasheet-c78-739512.html.

For information about Cisco Wireless software releases that support specific Cisco access point modules, see the "Software Release Support for Specific Access Point Modules" section in the *Cisco Wireless Solutions Software Compatibility Matrix* document.

What's New in Release 8.10.105.0

This section provides a brief introduction to the new features and enhancements that are introduced in this release.

Note For complete listing of all the documentation published for Cisco Wireless Release 8.10, see the Documentation Roadmap:

https://www.cisco.com/c/en/us/td/docs/wireless/doc-roadmap/doc-roadmap-release-810.html

New Access Point Support

In this release, support is introduced for the following new access points:

- Cisco Catalyst 9130 Access Points (C9130AXI-x)
  - C9130AXI: VID 02 or earlier
- Cisco Catalyst 9120AXE Access Points (C9120AXE-x) and Cisco Catalyst 9120AXP Access Points (C9120AXP-x)
  - C9120AXE: VID 06 or earlier
  - C9120AXP: All VIDs
- Cisco Aironet 1840 Series Access Points
- Cisco Catalyst IW6300 Heavy Duty Series Access Points
- Cisco 6300 Series Embedded Services Access Points

Wi-Fi 6 Features

OFDMA Download and Upload: Indroduced support in Cisco Catalyst 9130 APs.

MU-MIMO Download: Indroduced support in Cisco Catalyst 9130 APs.

High Efficiency (HE) Rates: Indroduced support in Cisco Catalyst 9130 APs.

Note For more information about feature support in 802.11ax APs, see Feature Matrix for Cisco Wave 2 Access Points and Wi-Fi 6 (802.11ax) Access Points.

Mesh Mode Support in Cisco Wave 2 Access Points

Mesh mode is supported in the following Cisco Wave 2 APs in this release:

- Cisco Aironet 1815 Series Access Points
- Cisco Aironet 2800 Series Access Points
- Cisco Aironet 3800 Series Access Points
- Cisco Aironet 4800 Series Access Points
- Cisco Catalyst IW6300 Heavy Duty Series Access Points
- Cisco 6300 Series Embedded Services Access Points

Note Mesh mode works only on those Cisco Aironet 2800 and 3800 Series APs that have been manufactured in the year 2017 or a later date.

To know the manufacturing date of your AP, enter the **show version** command on the AP console. The output of the command shows the *Top Assembly Serial Number*. A sample output is shown below:

```
Top Assembly Serial Number           : xxx2234xxxx
```

In the above example, the year code is 22, which is comprised of Base 10 numeric characters and is defined as *last two digits of the year + 4*. Therefore, if the manufacturing year is 2017, the year code is 21; if the manufacturing year is 2018, the year code is 22; and so on. The next two digits represent the calendar week of that year. In this example, the manufacturing date is the year 2018 and week number 34.

This restriction is not applicable to Cisco Aironet 1815 and 4800 Series Access Points.

Note Mesh mode was already supported in Cisco Aironet 1540 and 1560 Series APs prior to this release. For more information about the features supported on various Cisco Wave2 APs, see the *Feature Matrix for Cisco Wave 2 Access Points and Wi-Fi 6 (802.11ax) Access Points* at:

https://www.cisco.com/c/en/us/td/docs/wireless/access_point/wave2-ap/feature-matrix/b-wave2-ap-feature-matrix.html

Air Time Fairness Support in Cisco Wave 2 Access Points

Air Time Fairness (ATF) is supported in the following Cisco Wave 2 APs:

- Cisco Aironet 2800 Series Access Points
- Cisco Aironet 3800 Series Access Points
- Cisco Aironet 4800 Series Access Points
- Cisco Aironet 1560 Series Outdoor Access Points
- Cisco Catalyst IW6300 Heavy Duty Series Access Points
- Cisco 6300 Series Embedded Services Access Points

ATF is also supported in APs operating in mesh and Mobility Express modes.

For more information, see the *Feature Matrix for Cisco Wave 2 Access Points and Wi-Fi 6 (802.11ax) Access Points* at:

https://www.cisco.com/c/en/us/td/docs/wireless/access_point/wave2-ap/feature-matrix/b-wave2-ap-feature-matrix.html

Intelligent Capture Support Update

Support for the Intelligent Capture feature is added in the following APs:

- Cisco Aironet 1800 Series Access Points
- Cisco Catalyst 9115 Access Points

- Cisco Catalyst 9117 Access Points
- Cisco Catalyst 9120 Access Points
- Cisco Catalyst IW6300 Heavy Duty Series Access Points
- Cisco 6300 Series Embedded Services Access Points

The Intelligent Capture feature provides support to have a direct communication link between Cisco DNA Center and APs, so that each of the APs can communicate with Cisco DNA Center directly. Using this channel, Cisco DNA Center can receive packet capture data, AP and client statistics, and spectrum data.

For more information about configuring the Intelligent Capture feature, see the applicable *Cisco DNA Center Assurance User Guide* at

https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/products-user-guide-list.html

Cisco Access Points as Sensors is Not Recommended

Starting with Release 8.10, we recommend that you do not configure Cisco APs in sensor mode.

WPA3

WPA3 is a replacement to WPA2, as announced by the Wi-Fi Alliance. The new standard has two modes:

- **WPA3-Personal with 128-bit encryption**: The WPA3 standard provides a replacement to WPA2's preshared key (PSK) with Simultaneous Authentication of Equals (SAE), as defined in the IEEE 802.11-2016 standard. With SAE, the user experience is the same (choose a passphrase to connect), but SAE automatically adds a step to the *handshake*, which makes brute force attacks ineffective. With SAE, the passphrase is not exposed, making it impossible for attackers to find the passphrase through brute force dictionary attacks.

  The Protected Management Frames (PMF) should be used for all WPA3-Personal connections. Previously, PMF was an optional capability, which you could configure. With WPA3, PMF must be negotiated for all WPA3 connections that provide an additional layer of protection from deauthentication and dissociation attacks.

- **WPA3-Enterprise with 192-bit encryption**: This WPA3 standards is aligned with the recommendations from the Commercial National Security Algorithm (CNSA) Suite, which is commonly in place in high-security Wi-Fi networks in verticals such as government, defense, finance, and so on.

For more information about WPA3, see the Wi-Fi Alliance's website.

Enhanced Open

The Enhanced Open feature is based on Opportunistic Wireless Encryption (OWE) and provides encryption to open (unencrypted) wireless networks and a higher level of security against passive sniffing and simple attacks compared to a public PSK wireless network.

With Enhanced Open, clients and the controller or the AP perform a Diffie-Hellman key exchange during the access procedure and use the resulting pairwise secret with the 4-way handshake.

Enhanced Open requires no special configuration or user interaction.

For more information about Enhanced Open, see the the Wi-Fi Alliance's website.

Guidelines and Restrictions on WPA3

- WPA3 is not supported in Cisco Wave 1 (IOS-based) APs.
- IPSK with SAE is not supported.
- FT with SAE is not supported.
- Policy details for client joining WPA2+WPA3 WLANs:
  - Client policy is shown as WPA3 for personal security WLAN with SAE in enabled state.
  - Client policy is shown as WPA3 for Enhanced Open WLANs.
  - Client policy is shown as WPA3 only if client joining the WLAN has PMF in enabled state, has SUITE192-1x AKM, GCMP256 cipher, and the WLAN has WPA3 in enabled state. Else, the client policy is shown as WPA2.

For more information about configuring WPA3, see

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-10/config-guide/b_cg810/wlan_security.html#wpa3

This section contains the following subsections:

Agile Multiband

This feature is a Wi-Fi standard technology which manages the available Wi-Fi network resources optimally. The Wi-Fi Alliance Agile Multiband (MBO) feature supporting devices share information among each other to take better roaming decisions, provide better overall performance and experience to the user.

Support for –P Domain for Cisco Wireless LAN Solutions

The Cisco Wireless LAN Solution supports –P domain for Japan.

For the current approvals and regulatory domain information see https://www.cisco.com/c/dam/assets/prod/wireless/wireless-compliance-tool/index.html

Support for Trap Notification through SNMPv3

SNMPv3 for trap messages is now supported on controllers. For more information about configuring SNMPv3 for trap messages, see

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-10/config-guide/b_cg810/wireless_intrusion_detection_system.html#snmp-cli

Access Point Accounting

Prior to this release, there was no mechanism for RADIUS servers to monitor a network (apart from clients), specifically with respect to access points. If there were any network issues and APs repeatedly join and disjoin from the controller, there was no mechanism to monitor these events.

In this release, you can enable AP events to be forwarded to those RADIUS servers that are configured for management accounting. This ensures monitoring of these events to help you detect any network issues.

For more information, see

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-10/config-guide/b_cg810/aaa_administration.html#config-radius-acct-servers

Password Encryption

Controllers encrypt most of the passwords that are stored in the configuration file, using Advanced Encryption Standard-128 (AES-128). The encryption is hardcoded. To choose between the encrypted or the plain text method of storing passwords, use this command:

config switchconfig secret-obfuscation {**enable** | **disable**}

With secret obfuscation in enabled state, all the secrets from plain text are converted to encrypted values by using the hard-coded encryption key. This type of encryption is called type-7 encryption. If you disable secret obfuscation, all the secrets are converted from encrypted values to plain text passwords by using hard-coded encryption key. This type of encryption is called type-0 encryption. Secret obfuscation is enabled by default.

A disadvantage with type-7 encryption is that the passwords can be recovered from the hard-coded key value. There is a need for a stronger encryption method in which the key value can be configured. After you configure secret obfuscation, you can provide an extra level of encryption method that is called type-6. The type-6 method of encryption takes the configurable key along with AES-128 and stores the passwords. This stores all the secrets along with the configurable master key. You can change the key value from time to time to avoid decryption of passwords.

By default, type-6 encryption and password encryption are disabled.

The master key is encrypted with a device certificate private key. The master key length should be between 16 to 127 alphanumeric characters. We recommend that you use at least three of the following four classes in the password:

- Lowercase letters
- Uppercase letters
- Digits
- Special characters

The following applications use the type-6 encryption method:

- Local Net user
- RADIUS (Authentication, Accounting, and DNS)
- TACACS+ (Authentication, Accounting, Authorization, and DNS)
- IPSec secrets
- LDAP
- Local EAP
- SXP
- WPA2 PSK
- Local management user

This section contains the following subsections:

For more information, see

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-10/config-guide/b_cg810/managing_configuration.html#password-encryption

Per AP Group NTP Server

Features such as Hyperlocation require precise time across APs within an AP group to achieve location accuracy. Before Release 8.10, a controller synchronized with a global NTP server. By default, an AP synchronizes with the controller's time through periodic CAPWAP messages. If the DHCP server supplies an NTP server address via DHCP Option 42, the AP synchronizes with that server. The per AP group NTP server configuration takes precedence over the DHCP-configured NTP server. The DHCP server cannot override the AP group NTP server.

As controllers and controller global NTP server are configured on the WAN, they might have large synchronization delays from the AP, and this might compromise location accuracy.

The primary NTP server requirement is that all APs in an AP group synchronize with the same server.

For Hyperlocation and BLE AoA features, all APs in an AP group are required to synchronize with the same NTP server, such that the collected data can be used to calculate the location accurately.

Before Release 8.10, a Hyperlocation-specific per-AP group NTP server configuration which allowed for only IPv4 address format without authentication was supported. If you enabled the Hyperlocation feature, the AP used the Hyperlocation-specific NTP server configuration information to synchronize with specified NTP server. In case of failures, the AP fell back to the controller's time-sync mechanism. However, there are security risks if APs and the controllers access the same NTP server.

To address the requirements for these two sets of NTP server configuration to be independent of each other, you can configure a per-AP group NTP server in the controller.

The Hyperlocation-specific NTP server configuration is no longer available; you must configure the per-AP group NTP server separately.

For more information, see

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-10/config-guide/b_cg810/configuring_ap_groups.html#per-ap-group-ntp-server

This section contains the following subsections:

Software Release Types and Recommendations

Table 2: Release Types

Release Type	Description	Benefit
Maintenance Deployment (MD)	Software releases that provide bug-fix support and ongoing software maintenance. These releases are categorized as Maintenance Deployment (MD). These releases are long-living releases with ongoing software maintenance.	Provides you with a software release that offers stability and long support duration with periodic maintenance releases (MRs).
Early Deployment (ED)	Software releases that provide new features and new hardware platform support in addition to bug fixes. These releases are categorized as Early Deployment (ED). These releases are short-lived releases.	Allows you to deploy the latest features and new hardware platforms or modules.

For detailed release recommendations, see the *Guidelines for Cisco Wireless Software Release Migration Bulletin* at:

http://www.cisco.com/c/en/us/products/collateral/wireless/8500-series-wireless-controllers/bulletin-c25-730741.html.

Table 3: Upgrade Path to Cisco Wireless Release 8.10.x

Current Software Release	Upgrade Path to Release 8.10.x
8.5.x	You can upgrade directly to Release 8.10.x.
8.6.x	You can upgrade directly to Release 8.10.x.
8.7.x	You can upgrade directly to Release 8.10.x.
8.8.x	You can upgrade directly to Release 8.10.x.
8.9.x	You can upgrade directly to Release 8.10.x.

Upgrading Cisco Wireless Release

This section describes the guidelines and limitations that you must be aware of when you are upgrading the Cisco Wireless release and the procedure to upgrade.

Guidelines and Limitations

- An existing WLAN with *?* in its name continues to be supported with this upgrade. However, you cannot include *?* in the name when creating a new WLAN.
- If an AP locks out the console due to default management user credentials, you must configure the controller AP global credential with non-default username and password to get access to the AP console.
- WPA3 upgrade and downgrade guidelines:
  - If you downgrade from Release 8.10 to Release 8.5, if any AKM for SAE is configured, the AKM validation fails after the downgrade. The security is set to WPA2 and AKM to 802.1X. However, PMF configuration is retained, which results in an error.
  - FT set to enabled state and PMF set to Required state is allowed in Release 8.10 because PMF and FT configurations are decoupled. However, in Release 8.5, this configuration invalid. Therefore, upon downgrading to Release 8.5, the WLAN might be disabled.
  - If you want to upgrade from Release 8.5 to 8.10 and have WPA1 configured with none of the WPA1 AKM that are valid for Release 8.10, the WPA1 configuration is disabled after the upgrade because it impacts the status of the WLAN. Valid AKM for WPA1 in Release 8.5 are 802.1X, PSK, and CCKM.
- Software downgrade guidelines for Release 8.10:
  - If you plan to downgrade the Cisco controller from Release 8.10 software, we recommend you to downgrade to Release 8.5.151.0 or later to prevent the controller configuration files from being corrupted.
  - If you have configured new country codes in Release 8.10 and if you plan to downgrade to an earlier release, then we recommend that you remove the new country code configurations prior to the downgrade. For more information, see CSCvq91895.
- Before downgrading or upgrading the Cisco Controller to another release check for APs or AP modes support. Ensure that only supported APs are connected and also the APs are moved to supported modes on the release that the controller is upgraded or downgraded to.
- Legacy clients that require RC4 or 3DES encryption type are not supported in Local EAP authentication.
- If you downgrade to Release 8.0.140.0 or 8.0.15x.0, and later upgrade to a later release and and also have the multiple country code feature configured, then the configuration file could get corrupted. When you try to upgrade to a later release, special characters are added in the country list causing issues when loading the configuation. For more information, see CSCve41740.

Note Upgrade and downgrade between other releases does not result in this issue.

- After downloading the new software to the Cisco APs, it is possible that a Cisco AP may get stuck in an upgrading image state. In such a scenario, it might be necessary to forcefully reboot the controller to download a new controller software image or to reboot the controller after the download of the new controller software image. You can forcefully reboot the controller by entering the **reset system forced** command.

- It is not possible to download some of the older configurations from the controller because of the Multicast and IP address validations. See the "Restrictions on Configuring Multicast Mode" section in the *Cisco Wireless Controller Configuration Guide* for detailed information about platform support for global multicast and multicast mode.

- When a client sends an HTTP request, the controller intercepts it for redirection to the login page. If the HTTP GET request that is intercepted by the controller is longer than 2000 bytes, the controller drops the packet. Track the Caveat ID CSCuy81133 for a possible enhancement to address this restriction.
- When downgrading from one release to an earlier release, you might lose the configuration from your current release. The workaround is to reload the previous controller configuration files that are saved in the backup server, or to reconfigure the controller.
- When you upgrade a controller to an intermediate release, wait until all the APs that are associated with the controller are upgraded to the intermediate release before you install the latest controller software. In large networks, it can take some time to download the software on each AP.
- You can upgrade to a new release of the controller software or downgrade to an earlier release even if FIPS is enabled.
- When you upgrade to the latest software release, the software on the APs associated with the controller is also automatically upgraded. When an AP is loading software, each of its LEDs blinks in succession.
- Controllers support standard SNMP MIB files. MIBs can be downloaded from the software download page on Cisco.com.
- The controller software that is factory-installed on your controller and is automatically downloaded to the APs after a release upgrade and whenever an AP joins a controller. We recommend that you install the latest software version available for maximum operational benefit.
- Ensure that you have a TFTP, HTTP, FTP, or SFTP server available for the software upgrade. Follow these guidelines when setting up a server:
  - Ensure that your TFTP server supports files that are larger than the size of controller software image. Some TFTP servers that support files of this size are tftpd32 and the TFTP server within Cisco Prime Infrastructure. If you attempt to download the controller software image and your TFTP server does not support files of this size, the following error message appears:

    ```
    TFTP failure while storing in flash
    ```

  - If you are upgrading through the distribution system network port, the TFTP or FTP server can be on the same subnet or a different subnet because the distribution system port is routable.

- The controller Bootloader stores a copy of the active primary image and the backup image. If the primary image becomes corrupted, you can use the Bootloader to boot with the backup image.

  With the backup image stored before rebooting, from the **Boot Options** menu, choose **Option 2: Run Backup Image** to boot from the backup image. Then, upgrade with a known working image and reboot controller.

- You can control the addresses that are sent in the Control and Provisioning of Wireless Access Points (CAPWAP) discovery responses when NAT is enabled on the Management Interface, using the following command:

  config network ap-discovery nat-ip-only {**enable** | **disable**}

  The following are the details of the command:

enable—Enables use of NAT IP only in a discovery response. This is the default. Use this command if all the APs are outside the NAT gateway.

disable—Enables use of both NAT IP and non-NAT IP in a discovery response. Use this command if APs are on the inside and outside the NAT gateway, for example, Local Mode and OfficeExtend APs are on the same controller.

Note To avoid stranding of APs, you must disable the AP link latency (if enabled) before you use the disable option in the **config network ap-discovery nat-ip-only** command. To disable AP link latency, use the **config ap link-latency disable all** command.

- Do not power down the controller or any AP during the upgrade process. If you do this, the software image might get corrupted. Upgrading the controller with a large number of APs can take as long as 30 minutes, depending on the size of your network. However, with the increased number of concurrent AP upgrades supported, the upgrade time should be significantly reduced. The APs must remain powered, and controller must not be reset during this time.
- After you perform the following functions on the controller, reboot it for the changes to take effect:
  - Enable or disable LAG.
  - Enable a feature that is dependent on certificates (such as HTTPS and web authentication).
  - Add a new license or modify an existing license.

    Note Reboot is not required if you are using Right-to-Use licenses.

  - Increase the priority of a license.
  - Enable HA.
  - Install the SSL certificate.
  - Configure the database size.
  - Install the vendor-device certificate.
  - Download the CA certificate.
  - Upload the configuration file.
  - Install the Web Authentication certificate.
  - Make changes to the management interface or the virtual interface.

Upgrading Cisco Wireless Software (GUI)

Procedure

Step 1 Upload your controller configuration files to a server to back up the configuration files.

Note We highly recommend that you back up your controller configuration files prior to upgrading the controller software.

Step 2 Follow these steps to obtain controller software:

a) Browse to the Software Download portal at: https://software.cisco.com/download/home.
b) Search for the controller model.
c) Click **Wireless LAN Controller Software**.
d) The software releases are labeled as described here to help you determine which release to download. Click a controller software release number:

- Early Deployment (ED)—These software releases provide new features and new hardware platform support as well as bug fixes.
- Maintenance Deployment (MD)—These software releases provide bug fixes and ongoing software maintenance.
- Deferred (DF)—These software releases have been deferred. We recommend that you migrate to an upgraded release.

e) Click the filename <*filename.aes*>.
f) Click **Download**.
g) Read the Cisco End User Software License Agreement and click **Agree**.
h) Save the file to your hard drive.
i) Repeat steps *a* through *h* to download the remaining file.

Step 3 Copy the controller software file <*filename.aes*> to the default directory on your TFTP, FTP, SFTP, or USB server.

Step 4 (Optional) Disable the controller 802.11 networks.

Note For busy networks, controllers on high utilization, and small controller platforms, we recommend that you disable the 802.11 networks as a precautionary measure.

Step 5 Choose **Commands** > **Download File** to open the **Download File to Controller** page.

Step 6 From the **File Type** drop-down list, choose **Code**.

Step 7 From the **Transfer Mode** drop-down list, choose **TFTP**, **FTP**, **SFTP**, **HTTP**, or **USB**.

Step 8 Enter the corresponding server details as prompted.

Note Server details are not required if you choose HTTP as the transfer mode.

Step 9 Click **Download** to download the software to the controller.

A message indicating the status of the download is displayed.

Note Ensure that you choose the **File Type** as **Code** for both the images.

Step 10 After the download is complete, click **Reboot**.

Step 11 If you are prompted to save your changes, click **Save and Reboot**.

Step 12 Click **OK** to confirm your decision to reboot the controller.

Step 13 If you have disabled the 802.11 networks, reenable them.

Step 14 (Optional) To verify that the controller software is installed on your controller, on the controller GUI, click **Monitor** and view the **Software Version** field under **Controller Summary**.

CIMC Utility Upgrade for 5520 and 8540 Controllers

The AIR-CT5520-K9 and AIR-CT8540-K9 controller models are based on Cisco UCS server C series, C220 and C240 M4 respectively. These controller models have CIMC utility that can edit or monitor low-level physical parts such as power, memory, disks, fan, temperature, and provide remote console access to the controllers.

We recommend that you upgrade the CIMC utility to a version that has been certified to be used with these controllers. Controllers that have older versions of CIMC installed are susceptible to rebooting without being able to access FlexFlash, with the result that the manufacturing certificates are unavailable, and thus SSH and HTTPS connections will fail, and access points will be unable to join. See: CSCvo33873. The recommended versions addresses the vulnerability tracked in CSCvo01180 caveat.

The certified CIMC images are available at the following locations:

Table 4: CIMC Utility Software Image Information

Controller	Current CIMC Version	Recommended CIMC Version	Link to Download the CIMC Utility Software Image
Cisco 5520 Wireless Controller Cisco 8540 Wireless Controller	2.x	3.0(4r)	https://software.cisco.com/download/home/286281345/type/283850974/release/3.0(4r) **Note** We recommend you to upgrade the firmware from 2.0(13i) to 3.0(4r) using TFTP, SCP protocols only.
Cisco 5520 Wireless Controller Cisco 8540 Wireless Controller	3.0(4d)	3.0(4r)	https://software.cisco.com/download/home/286281345/type/283850974/release/3.0(4r)
Cisco 5520 Wireless Controller Cisco 8540 Wireless Controller	4.0(1a)	4.0(2n)	https://software.cisco.com/download/home/286281345/type/283850974/release/4.0(2n)

Table 5: Firmware Upgrade Path to 4.x version

Current Firmware Version	Upgrade Path to 4.x version
2.x	You must upgrade to a 3.x version and then upgrade to the recommended 4.x version.
3.x	You can upgrade directly to the recommended 4.x version.

- For information about upgrading the CIMS utility version 2.x , see the *Introduction to Cisco IMC Secure Boot* section in the *Cisco UCS C-Series Servers Integrated Management Controller CLI Configuration Guide, Release 3.0*:

  https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/sw/cli/config/guide/3_0/b_Cisco_UCS_C-Series_CLI_Configuration_Guide_301/b_Cisco_UCS_C-Series_CLI_Configuration_Guide_201_chapter_01101.html#d92865e458a1635

  For information about upgrading the CIMS utility version 2.x using webUI , see the *Updating the Firmware* section https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/sw/gui/config/guide/3_0/b_Cisco_UCS_C-Series_GUI_Configuration_Guide_for_HTML5_Based_Servers_301/b_Cisco_UCS_C-Series_GUI_Configuration_Guide_207_chapter_01101.html#task_C137961E9E8A4927A1F08740184594CA.

Note When upgrading the firmware using the webUI method, you must select **Install Firmware through Remote Server** option when prompted in the webUI.

- For information about upgrading the CIMC utility, see the *Updating the Firmware on Cisco UCS C-Series Servers* chapter in the *Cisco Host Upgrade Utility 3.0 User Guide*:

  https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/sw/lomug/2-0-x/3_0/b_huu_3_0_1/b_huu_2_0_13_chapter_011.html

- **Updating Firmware Using the Update All Option**

  This section mentions specific details when using CIMC utility with Cisco 5520 or 8540 controllers. For general information about the software and UCS chassis, see *Release Notes for Cisco UCS C-Series Software, Release 3.0(4)* at:

  https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/release/notes/b_UCS_C-Series_Release_Notes_3_0_4.html

  Release Notes for Cisco UCS C-Series Software, Release 4.0(2) at:

  https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/release/notes/b_UCS_C-Series_RN_4_0_2.html

Table 6: Resolved Caveats for Release 4.0(2f)

Caveat ID	Description
CSCvn80088	NI-HUU fails to handle the special characters in the password of CIFS remote share

Table 7: Resolved Caveats for Release 3.0(4l)

Caveat ID	Description
CSCvp41543	SSH weak KeyExchange algorithm [diffie-hellman-group14-sha1] has to be removed

Interoperability with Other Clients

This section describes the interoperability of controller software with other client devices.

The following table describes the configuration that is used for testing the client devices.

Table 8: Test Bed Configuration for Interoperability

Hardware or Software Parameter	Hardware or Software Configuration Type
Release	8.10.x
Cisco Wireless Controller	Cisco 3504 Wireless Controller
Access Points	C9130, C9120
Radio	802.11ax (2.4 GHz or 5 GHz), 802.11ac, 802.11a, 802.11g, 802.11n (2.4 GHz or 5 GHz)
Security	Open, WPA3-SAE/OWE (WPA3 Supported Clients), WPA2+WPA3 (Mixed Mode) PSK (WPA2-AES), 802.1X (WPA2-AES)(EAP-PEAP)
RADIUS	Cisco ISE 2.3, Cisco ISE 2.2
Types of tests	Association, Traffic (TCP/UDP/ICMP) and Roaming between Aps

The following table lists the client types on which the tests were conducted. Client types included laptops, handheld devices, phones, and printers.

Table 9: Client Types

Client Type and Name	Driver / Software Version
Wi-Fi 6 Devices (Mobile Phone and Laptop)	
Samsung Galaxy S10+	Android 9.0
Samsung S10 (SM-G973U1)	Android 9.0 (One UI 1.1)
Samsung S10e (SM-G970U1)	Android 9.0 (One UI 1.1)
Apple iPhone 11	iOS 13.2.1
DELL Latitude 5491 (Intel AX200)	Windows 10 Pro (21.40.2)
Laptops	

Client Type and Name	Driver / Software Version
Acer Aspire E 15 E5-573-3870 (Qualcomm Atheros QCA9377)	Windows 10 Pro (12.0.0.832)
Apple Macbook Air	OS Sierra v10.12.2
Apple Macbook Air 11 inch	OS X Yosemite 10.10.5
Apple Macbook Air 11 inch	OS Sierra 10.12.6
Apple Macbook Air 13 inch	OS High Sierra 10.13.4
Apple Macbook Pro	OS X 10.8.5
Macbook Pro Retina	OS Mojave 10.14.3
Macbook Pro Retina 13 inch early 2015	OS Mojave 10.14.3
DELL Latitude 3480 (Qualcomm DELL wireless 1820)	Win 10 Pro (12.0.0.242)
DELL Inspiron 15-7569 (Intel Dual Band Wireless-AC 3165)	Windows 10 Home (18.32.0.5)
DELL Inspiron 15-7569 (Intel Dual Band Wireless-AC 3165)	Windows 10 Home (18.32.0.5)
DELL Inspiron 13-5368 Signature Edi (Intel Dual Band Wireless AC 3165	Win 10 Home (18.40.0.12)
DELL Latitude E5430 (Intel Centrino Advanced-N 6205)	Windows 7 Professional (15.18.0.1)
DELL Latitude E5540 (Intel Dual Band Wireless AC7260)	Windows 7 Professional (21.10.1)
DELL Latitude E6840 (Broadcom Dell Wireless 1540 802.11 a/g/n)	Windows 7 Professional (6.30.223.215)
DELL Latitude 3480 (Qualcomm DELL wireless 1820)	Win 10 Pro (12.0.0.242)
DELL XPS 12 v9250 (Intel Dual Band Wireless AC 8260)	Windows 10 (19.50.1.6)
DELL XPS 12 9250 (Intel Dual Band Wireless AC 8260)	Windows 10 Home (21.40.0)
FUJITSU Lifebook E556 Intel 8260 (Intel Dual Band Wireless AC 8260)	Windows 8 (19.50.1.6)
Lenovo Thinkpad Yoga 460 (Intel Dual Band Wireless-AC 9260)	Windows 10 Pro (21.40.0)
Note For clients using Intel wireless cards, we recommend you to update to the latest Intel wireless drivers if advertised SSIDs are not visible.	
Tablets	
Apple iPad Air MD785LL/A	iOS 11.4.1

Client Type and Name	Driver / Software Version
Apple iPad Air 2 MGLW2LL/A	iOS 10.2.1
Apple iPad Air2 MGLW2LL/A	iOS 12.4.1
Apple iPad MD328LL/A	iOS 9.3.5
Apple iPad MD78LL/A	iOS 11.4.1
Apple iPad MGL12LL/A	iOS 9.1
Apple iPad mini 2 ME279LL/A	iOS 11.4.1
Apple iPad mini 2 ME279LL/A	iOS 12.0
Apple iPad mini 4 9.0.1 MK872LL/A	iOS 11.4.1
Apple iPad 2 MC979LL/A	iOS 9.3.1
Samsung Galaxy Tab A SM T350	Android 5.0.2
Samsung Galaxy Tab GT N5110	Android 4.4.2
Samsung Galaxy Tab SM-P 350	Android 6.0.1
Samsung Tab Pro SM-T320	Android 4.4.2
Toshiba Tab AT100	Android 4.0.4
Mobile Phones	
Apple iPhone 5	iOS 10.3.12
Apple iPhone 5c	iOS 10.3.3
Apple iPhone 7 MN8J2LL/A	iOS 11.2.5
Apple iPhone 8 plus	iOS 12.4.1
Apple iPhone 8 Plus MQ8D2LL/A	iOS 12.4.1
Apple iPhone MD237LL/A	iOS 9.3.5
Apple iPhone SE MLY12LL/A	iOS 11.3
Apple iPhone X MQA52LL/A	iOS 13.1
ASCOM Myco2	Build 2.1
ASCOM Myco2	Build 4.5
ASCOM Myco 3 v1.2.3	Android 8.1
ASUS Nexus 7	Android 6.0
AT100	Android 4.0.4
Drager Delta	VG9.0.2
Drager M300.3	VG2.4
Drager M300.4	VG2.4
Drager M540	DG6.0.2 (1.2.6)

Client Type and Name	Driver / Software Version
Google Pixel	Android 10
Google Pixel 3	Android 10
HTC One 6.0	Android 5.0.2
Huawei Mate 20 pro	Android 8.1
Huawei P20 Pro	Android 8.1
Huawei P7-L10	Android 4.4.2
LG v40 ThinQ	Android 9.0
Moto X 2nd gen	Android 5.0
Samsung Galaxy Mega GT-i9200	Android 4.4.2
Samsung Galaxy S10.P.1.4	Android 9
Samsung Galaxy S4	Android 4.2.2
Samsung Galaxy S7	Android 6.0.1
Samsung Galaxy S7 SM - G930F	Android 8.0
Samsung Galaxy S8	Android 8.0
Samsung Galaxy S9+ - G965U1	Android 9.0
Samsung Galaxy SM - G950U	Android 7.0
Sony Experia	Android 9.0
Spectralink 8440	Android 5.0.0.1079
Spectralink 8742	Android 5.1.1
Spectralink 8744	Android 5.1.1
Spectralink Versity Phones 9540	Android 8.1
Vocera Badges B3000n	4.3.1.17
Vocera Smart Badges V5000	5.0.2.163
Zebra MC40	Android Ver: 4.4.4
Zebra MC40N0	Android Ver: 4.1.1
Zebra MC55A	Windows 6.5
Zebra MC75A	OEM ver 02.37.0001
Zebra MC9090	Windows Mobile 6.1
Zebra MC92N0	Android Ver: 4.4.4
Zebra TC51	Android Ver: 6.0.1
Zebra TC52	Android Ver: 8.1.0
Zebra TC55	Android Ver: 8.1.0

Client Type and Name	Driver / Software Version
Zebra TC57	Android Ver: 8.1.0
Zebra TC8000	Android Ver: 4.4.3
Printers	
Zebra QLn320 Printer	LINK OS 6.0 v68.20.15Z
Zebra ZD410 Printer	LINK OS 6.0 v84.20.18Z
Zebra ZQ310 Printer	LINK OS 6.0 v68.20.15Z
Zebra ZQ610 Printer	LINK OS 6.0 v84.20.18Z
Zebra ZQ620 Printer	LINK OS 6.0 v85.20.19Z
Zebra ZT230 Printer	LINK OS 6.0 v72_20_18Z
Zebra ZT410 Printer	LINK OS 6.0 v84.20.18Z

Key Features Not Supported in Controller Platforms

This section lists the features that are not supported on various controller platforms:

Note In a converged access environment that has controllers running AireOS code, High Availability Client SSO and native IPv6 are not supported.

Key Features Not Supported in Cisco 3504 Wireless Controller

- Cisco WLAN Express Setup Over-the-Air Provisioning
- Mobility controller functionality in converged access mode
- VPN Termination (such as IPsec and L2TP)

Key Features Not Supported in Cisco 5520 and 8540 Wireless Controllers

- Internal DHCP Server
- Mobility controller functionality in converged access mode
- VPN termination (such as IPsec and L2TP)
- Fragmented pings on any interface

Key Features Not Supported in Cisco Virtual Wireless Controller

- Cisco Umbrella
- Software-defined access

- Domain-based ACLs
- Internal DHCP server
- Cisco TrustSec
- Access points in local mode
- Mobility or Guest Anchor role
- Wired Guest
- Multicast

Note FlexConnect locally switched multicast traffic is bridged transparently for both wired and wireless on the same VLAN. FlexConnect APs do not limit traffic based on IGMP or MLD snooping.

- FlexConnect central switching in large-scale deployments

Note

- FlexConnect central switching is supported in only small-scale deployments, wherein the total traffic on controller ports is not more than 500 Mbps.
- FlexConnect local switching is supported.

- Central switching on Microsoft Hyper-V deployments
- AP and Client SSO in High Availability
- PMIPv6
- Datagram Transport Layer Security (DTLS)
- EoGRE (Supported only in local switching mode)
- Workgroup bridges
- Client downstream rate limiting for central switching
- SHA2 certificates
- Controller integration with Lync SDN API
- Cisco OfficeExtend Access Points

Key Features Not Supported in Access Point Platforms

This section lists the key features that are not supported on various Cisco Aironet AP platforms. For detailed information about feature support on Cisco Aironet Wave 2 and 802.11ax APs, see:

https://www.cisco.com/c/en/us/td/docs/wireless/access_point/wave2-ap/feature-matrix/b-wave2-ap-feature-matrix.html

Key Features Not Supported in Cisco Aironet 1800i, 1810 OEAP, 1810W, 1815, 1830, 1840, 1850, 2800, 3800, and 4800 Series APs

Table 10: Key Features Not Supported in Cisco Aironet 1800i, 1810 OEAP, 1810W, 1815, 1830, 1840, 1850, 2800, 3800, and 4800 Series APs

Operational Modes	• Autonomous Bridge and Workgroup Bridge (WGB) mode • Mesh mode **Note** Mesh mode is supported in Cisco Aironet 1815i, 1815m, 1830, 1850, 2800, 3800, and 4800 Series APs in Release 8.10. • LAG behind NAT or PAT environment
Protocols	• Full Cisco Compatible Extensions (CCX) support • Rogue Location Discovery Protocol (RLDP) • Telnet • Internet Group Management Protocol (IGMP)v3
Security	• CKIP, CMIC, and LEAP with Dynamic WEP • Static WEP for CKIP • WPA2 + TKIP **Note** WPA +TKIP and TKIP + AES protocols are supported.
Quality of Service	Cisco Air Time Fairness (ATF) **Note** ATF is supported in Cisco Aironet 2800, 3800, and 4800 Series APs in Release 8.10.
FlexConnect Features	• PPPoE • Multicast to Unicast (MC2UC) **Note** VideoStream is supported • Traffic Specification (TSpec) • Cisco Compatible eXtensions (CCX) • Call Admission Control (CAC) • VSA/Realm Match Authentication • SIP snooping with FlexConnect in local switching mode

Note For Cisco Aironet 1850 Series AP technical specifications with details on currently supported features, see the Cisco Aironet 1850 Series Access Points Data Sheet.

Key Features Not Supported in Cisco Aironet 1800i, 1810 OEAP, and 1810W Series APs

Table 11: Key Features Not Supported in Cisco Aironet 1800i, 1810 OEAP, and 1810W Series APs

Operational Modes	Mobility Express
FlexConnect Features	Local AP authentication
Location Services	Data RSSI (Fast Locate)

Key Features Not Supported in Cisco Aironet 1830, 1850, and 1815 Series APs

Table 12: Key Features Not Supported in Cisco Aironet 1830, 1850, and 1815 Series APs

Operational Modes	Mobility Express is not supported in Cisco 1815t APs.
FlexConnect Features	Local AP Authentication
Location Services	Data RSSI (Fast Locate)

Key Features Not Supported in Mesh Networks

- Load-based call admission control (CAC). Mesh networks support only bandwidth-based CAC or static CAC
- High availability (Fast heartbeat and primary discovery join timer)
- AP acting as supplicant with EAP-FASTv1 and 802.1X authentication
- AP join priority (Mesh APs have a fixed priority)
- Location-based services

Key Features Not Supported in Cisco Aironet 1540 Mesh APs

- Dynamic Mesh backhaul data rate.

Note We recommend that you keep the Bridge data rate of the AP as auto.

- Background scanning
- Noise-tolerant fast convergence

Key Features Not Supported on Cisco Aironet 1560 APs

- MAC Authentication FlexConnect Local Authentication
- Noise-tolerant fast convergence
- Static WEP

Key Features Not Supported on Cisco Catalyst IW6300 Heavy Duty Series AP and 6300 Series Embedded Services AP

- MAC Authentication FlexConnect Local Authentication
- Noise-tolerant fast convergence
- Static WEP

Unfixed and Fixed Issues in Release 8.10.190.0

Open Caveats

Table 13: Open Caveats

Caveat ID Number	Description
CSCvo10708	Cisco 2800, 3800 APs do not defer off-channel scanning when multicast transmission is active
CSCvo26193	WLC not sending radius authentication request for mac auth when other WLAN profile has local entry
CSCvp40627	Cisco controller fails to initiate 1x message
CSCvp86151	IOS APs radio reset with code 44, mostly seen on 2.4GHz radio
CSCvp86251	WLC does not forward or bridge DHCP REQUEST or DISCOVER for WLAN inherited Central DHCP clients
CSCvq14112	1832 AP showing up as "low power" when using a PWRINJ5
CSCvq27679	Radio reset due to pak count mismatch false detection in 1572AP
CSCvq71200	WLC Sent RST after TACACS authenticationn request cause login failed.
CSCvq74938	AP 3800 stopped working due to kernel panic
CSCvq80582	AP9120/9115: low throughput issues, legacy rates with PMF Required
CSCvq81388	Wave1 AP resetting 5GHz radio often with radio reset code 44, messages with "DTX marked with poison"
CSCvq83638	Wave 2 AP (1562) does not pass traffic in Ethernet Bridging Mode on 8.5.151

Caveat ID Number	Description
CSCvq95330	Wave 2 WGB does not send IAPP message in static IP config
CSCvr18534	8540 WLC stopped working - "Crash function not supported by this task: RRM-MGR-2_4-GRP"
CSCvr23173	AP9117 invalid radar detection on non-serving channel
CSCvr28017	WLC does not show -A regulatory domain for 5 GHz radio with country code PA (Panama)
CSCvr34683	WLC resets it's config to factory default after power-cycle
CSCvr36185	2800 series APs are using 802.11n rates with WPA+TKIP only WLAN
CSCvr43311	Unable to set syslog login level to all the APs "Unable to set the Log Trap level"
CSCvr46272	Web Auth is required when client move to another AP during 4-way handshake
CSCvr54605	9115 sending 2 reassoc-resp with different SN and size for flex local sw central auth roam
CSCvr61717	WGB Wired client is not getting IP when associating to AP - 9130
CSCvr62819	1815W running 8.9.111.0 & 8.10.104.148 in OEAP mode - wired traffic fails
CSCvr63895	9130/9120 - Some APs sometimes show Continuous TX on channel 48/56/153/144
CSCvr74254	AP 9117 - Incorrect client count reported on QBSS IE in beacons
CSCvt04565	SSH access to the controller is failing, stating protocol error occurred

Resolved Caveats

Table 14: Resolved Caveats

Caveat ID Number	Description
CSCvh68195	8.8: 5520 Tracebacks observed 0x135956f 0x135af79 0x1362144 0x12ee263 0x3ba6c07dff 0x7f4ede3a439d
CSCvj08531	Interop speed issue between IOS AP and Intel 7260 8260 6235 with SMPS Dynamic Mode
CSCvj81943	Cisco 1530 Series Access Point reloads unexpectedly
CSCvk57014	AP: Sometimes creates empty radio core files without any information
CSCvm19309	Cisco 8510 controller IMM configuration is not taking effect
CSCvm46237	Cisco 1562 radio1 operational status down for all channels in blocked lists not going back up
CSCvm49047	AP 3702 reloads unexpectedly on 8.3.143.0

Caveat ID Number	Description
CSCvm63736	Erratic multicast throughput
CSCvm66185	During AP Boot the AP sends 3 dhcp releases causing BAD_ADDRESS on Windows Server 2016
CSCvm68624	Cisco Wave 1 AP console display logs 'DTX DUMP'
CSCvm84001	8.8MR1- WLC is sending wrong nasid for Flexconnect Local switching Clients
CSCvm95330	Cisco controller ignores DBS Max Best Channel Width Allowed
CSCvn00847	Cisco 702W AP loses connection to Cisco controller
CSCvn03079	Redundancy config sync errors while freeing client black list entry
CSCvn04907	'Length 0' line is automatically set to line VTY
CSCvn06723	PI 3.4: Copy and Replace AP fails, a Radio is DISABLED on Source AP, but ENABLED on Destination AP
CSCvn09271	Disable EEE on 702w - Not properly supported
CSCvn15447	WLC not disabling signature IDs
CSCvn31768	WLC cLWebAuthWlanConfigTable OID is broken when MS-OPEN feature is enabled on one of the SSIDs
CSCvn41324	Standby WLC keeps unjoined AP statistics entry even if statistics is cleared on Active WLC
CSCvn42067	MAPs Client radio (slot 0) chanAutoCfg changes from CONFIG_AUTO to CONFIG_STATIC at random
CSCvn42083	Cisco WLC DP reloads unexpectedly due to IP Frag buckets running out
CSCvn47019	Cisco Wave 2 AP WGB - Ping test failure from WGB wired client after join test when valid IP exists
CSCvn59160	WLC logs "NMSP cloud service update. Received CMX service Link Check" even when CMX is not used
CSCvn88031	WLC uses lowest LDAP server index when configuring mutliple servers that have same IP/different OUs
CSCvn99809	Handling PAK scheduler during AID plumbing
CSCvo05889	Socket send operation has failed on the socket descripto seen in Active WLC during portfailover
CSCvo08995	SNMP - cRFStatusPeerUnitState returns incorrect value when WLC lost its peer.
CSCvo09245	WLC sends incomplete Accounting packets using client's MAC as username after FlexConnect AP failover

Caveat ID Number	Description
CSCvo09482	CISCO-LWAPP-AP-MIB: DEFVAL format incorrect for some objects
CSCvo18656	Several AP configurations are changed after switchover
CSCvo18663	'Native VLAN Inheritance' is changed after controller switchover
CSCvo24010	2.4 GHz Rogue clients stay in containment pending
CSCvo25646	Split ACLs not being saved in the APs after they reboot
CSCvo26217	Fabric Enabled Wireless: Cisco 5520 WLC does not reconnect to CP
CSCvo28521	All mesh 1532 APs flooding with "ar9300_check_key_cache_entry: WEP key length 0 too small"
CSCvo31548	Cisco IW3702 AP and 3702 AP WGB reloads unexpectedly on 15.3(3)JF9 with PEAP authentication
CSCvo35484	RTS threshold is zero in show CAPWAP client config; excessive RTS sent; client connectivity problems
CSCvo37232	WLC - configuration of some WLANs is not listed in 'show run-config'
CSCvo41224	1832/1852 Observing False RADAR detection in 20 Mhz
CSCvo42865	Cisco controller reloads unexpectedly at task 'TransferTask' while uploading WebAdmin certificate
CSCvo46081	WLC HA standby goes to maintenance mode with 'reset system both in 00:03:00'
CSCvo48239	WLC in Germany(DE) Country DCA Bandwidth Config failed for 40MHz or above
CSCvo51266	EAP TLS failure with WGB
CSCvo55603	Cisco 4800 series access points not requesting UPoE power when connected to Cisco 94xx switch.
CSCvo56563	AP still shows up in WLC GUI/CLI even though manually removed from switchport
CSCvo57350	Cisco 1852 AP LED blinks amber even while it is successfully serving clients
CSCvo59784	AP usage shows discrepancy through pages
CSCvo74306	Cisco 1815W APs: Per-user BW contract not working with web policy
CSCvo80444	Nearby AP name not showing for 5-GHz network
CSCvo91229	AP deauth client with reason 7 after success re-association due to 'Unknown Mn,calling delete'
CSCvo99565	Static IP clients in DHCP_REQD state pass traffic if WLAN IDs are configured randomly
CSCvp00688	Cisco 2800, 3800 AP radio reloads unexpectedly

Caveat ID Number	Description
CSCvp06909	Traceback, DOT11-2-RADIO_FAILED, Not Beaconing for too long, get_vap_mcast_q_len: invalid interface
CSCvp25089	Multicast Traffic stops working when enabling Inline Tagging on CTS with IOS AP
CSCvp30608	Cisco 1810 AP with data DTLS encryption drop out of order CAPWAP data packets
CSCvp33020	IOS AP stops forwarding multicast traffic under high load
CSCvp34186	Cisco 9120AP: kernel panic crash at select_task_rq_fair+0x2c/0x7d8
CSCvp36524	Authentication Error when shared secret is registered from GUI and this length is greater than 16
CSCvp40992	WLC requires reboot to update Authz shared secret when Authc shared secret is changed
CSCvp43376	IP Phone cannot associate after modify WLAN configure/profile, delete client, idle timeout etc.
CSCvp45146	Downstream packet drop on Cisco 1815 AP
CSCvp46449	Cisco controller reloads unexpectedly with task emweb
CSCvp48157	Cisco 1570 RAP intermittently drops broadcast packets
CSCvp48726	Unable to change autonomous AP data rates in GUI
CSCvp51377	Mobility AP-List not shown on the Peer until rebooted
CSCvp53747	LLDP traffic observed on 1815t.
CSCvp58062	1800 series AP Radio core dump due to beacon stuck FW hang
CSCvp59502	Controller reloads unexpectedly during de-authenticating client in multiple times[10-15] on UI page
CSCvp60641	RRM Auto RF grouping has to have the same WLC Leader for both bands or FRA is broken
CSCvp61350	Unable to erase IW3702 Autonomous AP configuration
CSCvp62492	AP2802/3802 keep sending igmpv2 packets to 224.0.0.1 using 10.128.128.128
CSCvp68494	Cisco 2800 AP reloads unexpectedly due to exception when having MU-MIMO clients in network
CSCvp69474	Cisco 1815w running 8.5.140.0 reloads unexpectedly generating capwapd core dumps
CSCvp70358	AP2802 reloads unexpectedly with watchdog process sxpd
CSCvp72309	Cisco 3800 AP stops passing traffic under client load Intel NIC 8260/8265 load in MU-MIMO deployment

Caveat ID Number	Description
CSCvp73800	AP wrongly set 'Channel Center Segment 0' to '42' in Assoc Resp while it is operating on CH144/80MHz
CSCvp78698	Cisco WLC reloads unexpectedly during mesh tree update
CSCvp79400	WLC 3504 8.5.135 Radius Attribute CUI sending '\n'
CSCvp82490	Syslog server floods with too many messages
CSCvp82616	AP 3800 transmitting 802.11n with WMM disabled on 2.4Ghz after a manual FRA switch
CSCvp82631	CleanAir sensor down due to mrvlfwd: d0: *** sensord died (src/ki_task.c:684/0) - slot 0 ***
CSCvp82961	AID cannot be freed 8.5.144.33 2800AP local mode
CSCvp91790	Cisco Wave2 AP WGB - Uplink does not get established when Wave2 AP root-ap is rebooted
CSCvp96611	WLC generating client traps without a session-id
CSCvq00175	Regarding "config rf-profile max-client-trap-threshold" and "config rf-profile trap-threshold clients"
CSCvq00819	SNMP set on AP3802 fails when assigning AP HA Pri/Sec on 8.5.144.0
CSCvq01837	Fabric Interface Name might not be shown on GUI
CSCvq04108	64-character RADIUS server Shared Secret in WLC gets corrupted after power cycle
CSCvq10242	Client obtains IPv6 link local address with IPv6 disabled
CSCvq22269	APs stuck in downloading state
CSCvq25317	PMIPv6 - WLC as MAG sends DHCP ACK with subnet mask 0.0.0.0 and router addr 0.0.0.0 on DHCP renewal
CSCvq25654	2702 AP Sent deauthentication to multicast MAC address
CSCvq26161	Update (1815M/1542) POE power request to match HW spec.
CSCvq26205	8.10 (WLC:3504): system reloads unexpectedly with task dx_sync_task
CSCvq26208	TX complete not happening for all frames [Tx stuck after 2 mins for 10 seconds]
CSCvq28024	AP3802I 2.4g band did not show correct Noise Information
CSCvq39469	9120: kernel panic: coredump: process ntp_proc; SW crashed on Process capwap_brain
CSCvq42724	WLC sends clients DHCP DISCOVER or REQUEST packets via wrong destination port UDP 68
CSCvq49277	Cisco 8540 controller reloads unexpectedly on Task name: emWeb

Caveat ID Number	Description
CSCvq52834	AP2800/3800/4800 doing CAC after radio up/down on DFS channel in Local Mode
CSCvq58748	Cisco 9115: Some commands are taking too long to respond
CSCvq59233	AP2802: Kernel panic crash: PC is at _Z27clickps_atomic_dec_and_testP8atomic_t
CSCvq60489	C9120AXI-B reloads unexpectedly due to kernel panic reason
CSCvq60744	HA SSO active WLC reloads unexpectedly due to apfReceiveTask
CSCvq63117	Client can not send the traffic, when two clients in different VNID joins the network
CSCvq64828	Radio stopped working on AP2800 and rcore was created
CSCvq67649	WLC - certain AP Airewave Director Configuration is not listed in 'show run-config'
CSCvq69068	IOS AP drops M2 when client is roaming
CSCvq70602	capwapd experiences watchdog timeout while trying to connect to cleanaird IPC socket
CSCvq71817	WLC OUI file incompatibility
CSCvq72812	Cisco Wave 2 APs dropping CAPWAP keepalive and unable to join 9800 WLC
CSCvq84949	AP9120 on DFS Channels not responding to probe request causing client join problems
CSCvq84965	AP9120 Click has the client stale entries in client IP table
CSCvq88525	AP2800 radio stopped working in newdp-dma-thread-stuck
CSCvq92184	Clients unable to connect to AP with data encryption enabled
CSCvq92379	AP9120 dual_dfs rmmod causes kernel crash
CSCvq92443	AP9120 Flooding "chatter: our own containing BSSID"
CSCvr01310	AireOS 8.x || MN country code Regulatory domain (-E) for Outdoor missing on WLC
CSCvr01652	CWA broken for SDA in 8.9
CSCvr01892	Cisco 2800 AP SW reloads unexpectedly on process hostapd
CSCvr07053	Lot of aptraced cores seen on production network with 16.12.1
CSCvr09722	Cisco 1832 APs: Association denied because AP is unable to handle additional associated STAs
CSCvr14071	3802 when CAPWAP resets, does not send disassociate
CSCvr14946	1815t CDP is not sent over WAN interface even after being enabled.
CSCvr27788	5GHz radio on 1562E-G APs Operationally Down - Regulatory Domain Failure when Pakistan is Configured
CSCvr29590	WLC local EAP does not send access-reject on auth failure

Caveat ID Number	Description
CSCvr35679	Flex LS, Central Authentication and Local Association - CCKM, roaming failure due to RN mis-match
CSCvr55000	C9120AX unable to pass traffic during throughput test
CSCvh86415	RADIUS server IP address showing wrong in Alarms UI
CSCvm57952	IPv6 clients struck with DHCP_REQD state with Local Switching webauth WLAN

Related Documentation

Wireless Products Comparison

- Use this tool to compare the specifications of Cisco wireless access points and controllers:

  https://www.cisco.com/c/en/us/products/wireless/wireless-lan-controller/product-comparison.html

- Product Approval Status:

  https://prdapp.cloudapps.cisco.com/cse/prdapp/jsp/externalsearch.do?action=externalsearch&page=EXTERNAL_SEARCH

- Wireless LAN Compliance Lookup:

  https://www.cisco.com/c/dam/assets/prod/wireless/wireless-compliance-tool/index.html

Cisco Wireless Controller

For more information about the controllers, lightweight APs, and mesh APs, see these documents:

- The quick start guide or the installation guide for your particular controller or access point
- Cisco Wireless Solutions Software Compatibility Matrix
- Cisco Legacy Wireless Solutions Software Compatibility Matrix
- Cisco Wireless Controller Configuration Guide
- Cisco Wireless Controller Command Reference
- Cisco Wireless Controller System Message Guide

For all controller software related documentation, see:

http://www.cisco.com/c/en/us/support/wireless/wireless-lan-controller-software/tsd-products-support-series-home.html

Cisco Mobility Express

- *Cisco Mobility Express Release Notes*
- *Cisco Mobility Express User Guide*
- *Cisco Aironet Universal AP Priming and Cisco AirProvision User Guide*

Cisco Aironet Access Points for Cisco IOS Releases

- *Release Notes for Cisco Aironet Access Points for Cisco IOS Releases*
- *Cisco IOS Configuration Guides for Autonomous Aironet Access Points*
- *Cisco IOS Command References for Autonomous Aironet Access Points*

Open Source Used in Controller and Access Point Software

Click this link to access the documents that describe the open source used in controller and access point software:

https://www.cisco.com/c/en/us/about/legal/open-source-documentation-responsive.html

Cisco Prime Infrastructure

Cisco Prime Infrastructure Documentation

Cisco Connected Mobile Experiences

Cisco Connected Mobile Experiences Documentation

Cisco Digital Network Architecture

https://www.cisco.com/c/en/us/support/wireless/dna-spaces/series.html

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you’re looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions, and services, visit Cisco DevNet.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.